

## enVision Security: Cyber Security Vulnerability Awareness Visualisations for Products



**Aneesha Sethi**  
**University of Southampton**

The substantial increase in the number of users of data services as a part of their everyday lives make them more vulnerable to cyber-attacks and give cyber criminals more incentives to exploit these services for potential gains.

These users are usually unaware of the security risks they face, which makes awareness about Cyber Security an extremely crucial topic for the present digital age. In order to protect data, one first has to be aware of the risks and vulnerabilities that the storage or processing of data may represent. Thus, this poster presents 'enVision Security', which is a solution to address this problem. It presents interactive data visualisations to present information about threats and vulnerabilities in products (like operating systems), in a way that is accessible to non-experts.

The web-based visualisations allow users to quantify the risks and threats in products by presenting it to them in a manner that is easy to grasp and retain by people. These visualisations have been created using real data to allow comparisons to be drawn between real products.

To evaluate the usefulness of this visualisation platform, a survey was presented to a random group of people to infer their experiences using the software. The success of the visualisation platform lay in the fact that 80% of the survey participants stated that they would use this system as it rose awareness about cyber security in an easy and interactive manner.

## CASTLE project

**Federica Paci**  
**University of Southampton**

The aim of CASTLE project is to increase student engagement and learning experience with cyber security practices while at the same time improving the adoption of cyber security practices in our academic environment. This poster reports how the student learning experience and a university's security posture has been enhanced through supervised penetration testing activities of university systems. In particular, the poster illustrates the design of a penetration testing framework and a virtual software platform to allow students to conduct penetration testing against University of Southampton IT services.

# Effectiveness of Digital Forensics Education & Training

**Georgina Humphries**  
**Canterbury Christ Church University**

This poster focusses on the ever evolving nature of the digital arena surrounding Cyber Security and Digital Forensics. Digital Forensics plays a crucial role in many criminal investigations with Cyber Security no longer being just a buzzword.

However, emphasis is placed on the development, and role of, courses within higher education (HE) and businesses across the United Kingdom. With this development, an effective national curriculum and training framework is increasingly necessary. Discourse surrounding integration of Computer Forensics has placed focus towards the teaching of Digital Forensics, but little in the way of collaboration amongst the community within the educational sector.

There is little assurance over the placement of such a multi-/interdisciplinary course, or its position within STEM subjects; where it has yet to define itself. An aspect of this study is to focus on the lack of a national framework and work on producing a framework while also focussing on the effectiveness of teaching and training a Digital Forensics practitioner.

## Open Source Internet Research Tool (OSIRT): an Investigative Tool for Law Enforcement Officials

**Joseph Williams**  
**Canterbury Christ Church University**

Open Source Internet Research Tool (OSIRT) is a self-described “browser on steroids” that’s designed to aid law enforcement officials of all skill-levels to conduct Open Source Research on the Internet.

OSIRT styles itself on the look-and-feel of a normal web browser, but provides additional functionality such as screen capturing and automated logging of webpages visited. All evidential artefacts are automatically placed into a case container, along with the date and time they were obtained and a cryptographic hash for file verification.

OSIRT has been designed in collaboration with the College of Policing, where it is used as a centre piece for one of the College’s training courses. In addition to this, OSIRT is also used by numerous law enforcement officials across the UK for live investigations; with many of OSIRT’s features based directly from law enforcement feedback and suggestions.

This poster highlights the current features of OSIRT, along with OSIRT’s future direction and a call for ideas and suggestions from the academic community.

## Cyber Security CPD for Industry Professionals

**Kieran McLaughlin**  
**Queen's University Belfast**

This project explores how best to offer innovative, flexible, and accessible ways to study cyber security for postgraduate industry professionals in the context of continuing workplace commitments.

It explored the opportunities for the development and online delivery of an advanced level cyber security course for part-time post graduate study. The project incorporated working collaboratively with industry partners and computer science students in the course design, production and delivery of cyber security learning resources.

This project sought to ensure the development, delivery, and evaluation of an online cyber security taught course that targets part time Post Graduate students.

Employees, at the project partner company Kainos, provided a pilot cohort of local, national and international students to work as partners and to actively engage in each stage of the project to ensure the course will enhance their learning experience and help inform best practice for the course design and delivery.